REMARKS/ARGUMENTS

Prior to the entry of this amendment, claims 1-15 were pending in this application. Claims 1, 10, and 11 have been amended herein. New claims 16-19 have been added and claims 8 and 9 have been canceled without prejudice. Therefore, claims 1-7 and 10-19 are pending in the application. Applicants respectfully request reconsideration of this application for at least the reasons presented below.

As required by the Office Action, Applicants have corrected the Abstract above by deleting the reference numbers.

Claim Objections Informalities

The Office Action has objected to claims 1-7 for informalities. Specifically, the Office Action has indicated that claim 1 recites the word "processing" twice. Applicants thank the Examiner for his careful reading of the claims and for pointing out this informality. Appropriate amendments have been made to claim 1 to correct this informality.

35 U.S.C. §103 Rejection, Lewis in view of Schneier

The Office Action has rejected claims 1-15 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,761,306 of Lewis (hereinafter "Lewis") in view of *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, of Schneier, Second Edition, pps. 183-184, 1996 (hereinafter Schneier). The Applicants respectfully submits that the Office Action does not establish a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicants requests reconsideration of these claims.

In order to establish a *prima facie* case of obviousness, the Office Action must establish: 1) some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or

combine their teachings; 2) a reasonable expectation of success of such a modification or combination; and 3) a teaching or suggestion in the cited prior art of each claimed limitation. See MPEP §706.02(j). However, the cited references fail to teach or suggest, alone or in combination, each claimed limitation.

Lewis "provides an active public key and a 'masked' replacement public key to nodes of a network." (Col. 3, lines 16-18) As used in Lewis, "'masked' or 'the mask of' refers to any manner of securing the replacement key so that it is computationally difficult to determine the replacement key from its masked version." (Col. 3, lines 18-21) "In one embodiment of [Lewis] the masking of the replacement key is accomplished by hashing the replacement public key." (Col. 3, lines 21-23) "In an alternate embodiment of [Lewis], the replacement public key is encrypted instead of using the hash of the replacement public key." (Col. 4, lines 13-15) However, Lewis says nothing about the length of the key(s) used to encrypt the replacement key relative to the replacement key(s). Lewis does point out that the a replacement key may be longer than the key that it is replacing. (Col. 7, lines 43-48) However, this still says nothing about the length, complexity, time to process, resources to process, etc. of the replacement key relative to that of the key used to process the replacement key.

The cited portion of Schnier discusses the lifetime of keys and the reasons for periodically replacing keys. However, the cited portion of Schnier does not discuss methods of performing key replacements. Therefore, the cited portion of Schnier also says nothing about the length, complexity, time to process, resources to process, etc. of the replacement key relative to that of the key used to process the replacement key.

Claim 1, upon which claims 2-7 and 11 depend, relates to a cryptographic processing system using a multiple key hierarchy. Claim1 recites in part "a first key for performing asymmetric operations at a first rate, wherein each operation requires a first cryptographic processing time; and a second key for performing an asymmetric cryptographic processing operation to update the first key, wherein the second key is used in cryptographic processing operations on the first key at a second rate that is less often than the first rate and that

requires a second cryptographic processing time greater than the first cryptographic processing time." Neither reference, alone or in combination, teaches or suggests the second key used in cryptographic processing operations on the first key where the second key requires a second cryptographic processing time greater than the first cryptographic processing time to process the first key. Rather, the cited portion of Schnier is completely silent in regards to methods or systems for replacing keys and Lewis says nothing about the time to perform operations with the first key, i.e., decrypt data using the replacement key, relative to the time to process the second key, i.e., decrypt the replacement key. For at least these reasons, claims 1-7 and 11 should be allowed.

Claim 10, upon which claims 12-15 depend, relates to a method for updating keys in a digital system used to transfer data. Claim 10 recites in part "a first asymmetrical cryptographically processed key to perform an asymmetric cryptographic processing operation to decode the information, wherein the cryptographic processing operation is at a first level of complexity requiring a first amount of resources . . . transferring a second asymmetrical cryptographically processed key to the digital processing device, wherein the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity requiring a second amount of resources by the processing device that is higher than the first amount of resources . . . [and] encoding a substitute first asymmetrical cryptographically processed key with a second key, so that the resulting cryptographically processed substitute first asymmetrical cryptographically processed key is decodable by the second asymmetrical cryptographically processed key." Neither reference, alone or in combination, teaches or suggests the second key for decoding the first key where the second key is at a level of complexity requiring more resources to process than the first key. Rather, the cited portion of Schnier is completely silent in regards to methods or systems for replacing keys and Lewis says nothing about the resource to process the first key, i.e., decrypt data using the replacement key, relative to the resources to process the second key, i.e., decrypt the replacement key. For at least these reasons, claims 10 and 12-15 should be allowed.

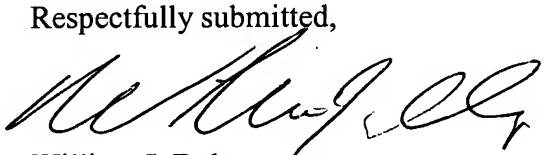
To obviate a rejection of new claims 16-19 it is noted that claim 16, upon which claims 17-19 depend, relates to a method of updating a cryptographic key used for decrypting distributed data and recites in part "generating a first key for decrypting the distributed data, the first key of a first length; encrypting the first key with a second key, the second key of a second length, wherein the second length is longer than the first length." Neither reference, alone or in combination, teaches or suggests encrypting the first key with a second key, the second key of a second length, wherein the second length is longer than the first length. Rather, the cited portion of Schnier is completely silent in regards to methods or systems for replacing keys and Lewis says nothing about the length of the key used to encrypt the replacement key relative to the length of the replacement key. For at least these reasons, claims 16-19 should be allowed.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,



William J. Daley
Reg. No. 52,471

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 303-571-4321

WJD:sbm

60618964 v1